Information rights report
Quarter 1 2016/17

Contents

1. Key Developments

Some key developments expected in the next quarter are:

- Adoption of EU-US Privacy Shield by the European Commission.
- Progression of the Digital Economy Bill through Parliament.
- ICO response to the House of Commons Culture Media and Sport Committee report Cyber security report to be published.
- ICO response to the consultation on the National Data Guardian's report on Health and Care Data Security and Consent.
- Publication of Big data report 2.0.

2. Cross Sectoral Work

Good Practice:

We are developing our communications strategy for the department in order to further effectively promote the work we do and share the outcomes of the work we have done. First steps will be to speak to all our stakeholders to get their feedback and ideas on what sort of information they would like to see.

Contact: Louise Byers

GDPR guidance

Following on from the '12 steps' guidance published in March, in early July the ICO published a comprehensive overview of the GDPR. The document was published with an introduction and accompanying blog on the ICO website, explaining why the GPDR is still relevant to UK organisations.

Contact: Steve Wood

External guidance

The ICO published replacement guidance on section 38 – health and safety. The changes include more examples from case work and tribunal decisions, and clarification on what endangering mental health means.

Contact: Jo Pedder

Technology

The following guidance is ready for publication in Q2:

- Cookies - an updated version of the existing ICO guidance is undergoing internal review
- Principle 7 - an update to the existing pages on Principle 7 in The Guide to Data Protection is undergoing internal review

The ICO responded to the European Commission's public consultation on the evaluation and review on the ePrivacy Directive. The ePrivacy Directive is transposed into UK law in the Privacy and Electronic Communications Regulations. This includes provisions on direct marketing, cookies and the security of the public telecommunications services. The ICO submission to the Commission set out the areas where the Directive could be reformed, including a move to opt-in as the default for marketing communications and where overlap with the GDPR could be addressed (data breach notification).

Within the Article 29 Working Party technology subgroup, the ICO has input into the opinion on the review of the ePrivacy Directive, employee monitoring and data protection impact assessments. The ICO is also participating within the EDPB IT Taskforce, a group of DPAs set-up to oversee the specification and delivery of an IT system for the European Data Protection Board.

A blog on passwords and the security of Internet of Things has also been prepared for publication. This was scheduled for publication within the quarter but has been delayed due to the coverage of the referendum result.

The Technology team also delivered presentations to ICO staff on blockchain and privacy-friendly tech alternatives.

Version 2.0 of the ICO report on big data has been drafted (the first version was published 2014) and will be published Q2. This has been developed after further research and discussions with stakeholders e.g insurance sector.

Contact: Simon Rice

Freedom of Information - Model Services Contract

More information should be available in future about the performance of government contracts worth over £10 million, thanks to changes to the Model Services Contract. Under the updated version, suppliers must provide 'transparency reports' to public authorities, including details of their performance and their major subcontractors, and the authority can then publish these.

The changes have come about as a result of widespread concerns about transparency regarding outsourcing. The ICO has contributed to the Institute for Government's (IfG) work on public sector contracts and a blog on the IfG website gives more detail about the changes. Last year we also called for more proactive publication in our Transparency in Outsourcing Roadmap and our guidance on outsourcing and FOI.

Contact: Steve Wood/Carl Wiper

3. Government and Society Sector

HMRC employment history subject access requests

NOT FOR PUBLICATION

Political parties and campaign groups

We have continued to receive enquiries about the Referendum campaign from individuals and others on a number of issues relating to the conduct of campaign organisations. These enquiries have included use of the full electoral register and also arrangements for lobbying individual electors.

Outcome:

We have met with the Cabinet Office Registration and Franchise Team to discuss the uses of both the full and open electoral registers and clarified the role of credit reference agencies in their provision of the electoral register to campaign organisations.

Future action:

We will be meeting jointly with the Cabinet Office and the Electoral Commission to review the data protection and privacy issues arising from the Referendum arrangements and process.

We also wish to explore with both the Cabinet Office and the Electoral Commission how the agreed formal form of words on registration documentation may be clarified and expanded to provide additional information to the public about the Open Register and how to opt out.

We will also wish to review what lessons should be learned from referendum and whether revisions to the ICO's campaigning guide are necessary

Contact: Judith Jones, Alexander Ganotis

Data sharing proposals, including pending legislation (Digital Economy Bill)

We have continued to engage with the Cabinet Office on its plans to make better use of government data. Following the publication of the Cabinet Office's consultation on better use of data in government at the end of February, the Government and Society team coordinated a substantial formal response to the consultation and proactively shared this on our website and with other engaged stakeholders involved in the earlier open policymaking process that had helped shape the eventual Cabinet Office

proposals. Following the submission of our consultation response in April, we have met the Cabinet Office on a bilateral basis to expand upon some aspects of our consultation response and hear more from them about the important safeguarding role envisaged for the ICO.

The Digital Economy Bill, which includes a section on the better use of data, had its first reading in parliament on 5 July. The Bill includes powers to allow data sharing for a number of purposes including Fuel Poverty; Research and Statistics; Fraud; Debt; General Register's Office (births and deaths). Regulatory Delivery, formerly known as the Better Regulation Delivery Office, continues to work with us on improving the draft version of the data sharing guidance for non-economic regulators.

Outcome:

In our consultation response in April, we welcomed the key guiding principles behind the Cabinet Office proposals, which included no building of new, large and permanent databases or collecting more data on citizens; no indiscriminate sharing of data within government; and no amending or weakening of the Data Protection Act. The version of the Digital Economy Bill introduced at first reading doesn't differ significantly in data sharing content from that which was proposed in the consultation. The Bill includes numerous safeguards - some in the form of codes of practice which requires ICO consultation and will reinforce the data protection principles and ICO good practice; others in the form of pilot projects that require evaluation at the end of the pilot period. The codes in particular will contribute to transparency due to their requirement to produce privacy impact assessments, and make these assessments available for public scrutiny. Some civil society groups were concerned about some of the proposals in the consultation earlier this year. We do not know yet whether these concerns have been adequately addressed in the Bill's version of the data sharing proposals.

Future work:

We shall continue to engage with the Cabinet Office as the proposals in the Digital Government section of the Digital Economy Bill develop. We will monitor the Bill's progress through parliament and stand ready to respond formally when a public bill committee is launched. We will remain alert to civil society concerns over the data sharing proposals and in particular whether their concerns expressed at the consultation stage persist.

We shall continue to provide advice to Regulatory Delivery as they develop the latest draft of their data sharing guide for non-economic regulators.

Contact: Judith Jones, Jonathan Bamford

Charity fundraising

NOT FOR PUBLICATION

4. Police, Justice and Borders Sector

Good Practice:

We have completed the first of three audits of the Metropolitan Police Service. The first audit covered requests for personal data and, as a result of the assurance that was offered in relation to their processes, the ICO have taken the decision to discontinue our formal monitoring of the Met's performance in relation to subject access requests.

We are in the process of completing the first in a series of audits with the Police Service of Scotland. We have also agreed to conduct an audit of Kent Police later in the year. Once these audits have been completed we will have audited all 43 UK police forces.

We have initiated projects to engage with Business Crime Reduction Partnerships, in partnership with the National Association of Business Crime Partnerships (NABCP), and Law Centres and are planning similar projects with Bluelight Services.

We have worked with the Communications department to raise awareness of our Advisory Visit service to the legal sector, with particular emphasis on solicitors and barristers. This has resulted in a number of visits being scheduled with organisations in that sector.

Contact: Louise Byers

Police use of surveillance technologies

NOT FOR PUBLICATION

Police National Computer

NOT FOR PUBLICATION

Investigatory Powers Legislation

NOT FOR PUBLICATION

Data Retention and Investigatory Powers Act / Data Retention Regulation duties

NOT FOR PUBLICATION

Home Office National Databases Project

NOT FOR PUBLICATION

Metropolitan Police Service

NOT FOR PUBLICATION

5. Public Services Sector

Good Practice:

We continue to work closely with umbrella organisations to promote the outcomes of our work including attending conferences, delivering workshops, promoting the self-assessment toolkit and using videos on our website for specific sectors covering some of the key DP themes that have been included in our programme of workshops.

As an example, we are working with the General Pharmaceutical Council (GPC) on a programme of work within the Pharmacy sector including the production of bespoke awareness and training material specifically for the sector, advisory visits and an online survey.

We have begun work on a series of projects across the public services sector, for example one looking at data protection compliance in the early years learning sector and one to survey governance arrangements within local authorities with a view to producing an outcomes/best practice report for the sector as a whole.

Contact: Louise Byers

High Profile Case - Care.data disclosure objections

Patients were offered the opportunity to object to Health and Social Care Information Centre (HSCIC now NHS Digital) sharing their personal data with other organisations. This is known as a 'type two' objection. This option was provided through household leaflet drops and there is currently a pause given concerns over the process. Patients who acted on the leaflets informed their GP who would then 'flag' the objection in their electronic record. As full Care.data extraction was not initiated the 'flags' have not been received by HSCIC and therefore data flows to third parties are taking place irrespective of these. There has been media coverage of this and we have received a complaint from a civil society organisation.

Concerns have also been raised with us about what are known as 'type one' objections which stop data going to the Care.data programme. The concern is that the 'flag' not only blocks the data flow from the GP to HSCIC for its purposes but from the GP to any other organisation for anything other than a patient's direct care like health screening appointments.

Outcome:

Although we secured an undertaking from the HSCIC to bring processing

into compliance with the DPA there have been significant developments. Following on from our involvement and the findings of the National Data Guardian for Health and Care (NDG) review, the care.data scheme has been formally discontinued by the Department for Health.

Future work:

Although the care.data scheme has been discontinued, the broad aim which it was intended to address is likely to be investigated further following the publication of the NDG review.

We will be working closely with NHS England, NHS Digital and others to ensure that any new proposals regarding the further use of patient data is compliant with the DPA.

Contact: Victoria Cetinkaya. Laura Booth (undertaking work)

Reviews on Health and Care Data Security and Consent

The Secretary of State for Health commissioned the NDG to review and produce a report on security and also detailing whether the NHS should offer an opt out of data being used for purposes other than direct care. We took part in the NDG review panel. The Care Quality Commission (CQC) was also commissioned to produce a report on data security. Both these reports have been published by the Secretary of State together.

The CQC report recognises that whilst there is widespread commitment to the security of patient data there are challenges in delivering in practice. It makes six general recommendations to improve matters.

The NDG review makes ten recommendations around security and further recommendations about establishing a new patient consent/opt out model. The Government will consult on these though has already stated it is supportive of the introduction of stronger criminal sanctions against those who use anonymised data to re-identify individuals.

The Government also published its response to an earlier consultation on the role of the NDG. The response includes numerous references to ICO evidence and aligns with our comments on the need for the ICO and NDG to work closely to provide effective regulation.

Outcome:

We played a significant part in the NDG review process including the opportunity to comment on the draft findings before publication and provide reactions on these particularly around the role of the ICO's Anonymisation Code of Practice. The final report reflected these later

comments and is consistent with the points made during the review process.

The Government's response on the results of its consultation exercise on the role of the NDG also reflects points made by us during that consultation including the need for cooperative working. A MoU with the NDG has already been drafted to this effect. The Government has committed to put the role of the NDG a statutory footing at the next available opportunity.

Future work:

Following the publication of the report, there is a further consultation being undertaken by the Department of Health into the issues of security standards and consent.

We will be responding to the consultation, as well as working with key stakeholders including NHS England and NHS Digital (HSCIC) on the recommendations in the two reports and Government's NDG proposals.

Health data has previously been identified by the ICO as one of its priority action areas. The recent reports and cessation of care.data programme may provide a sensible point to review our approach to an area that involves sensitive personal data, engages significant data protection concerns (such as with security breaches) and engages substantial public and media interest.

Contact: Stacey Egerton & Victoria Cetinkaya

New Models of Care

The present trend for increased data sharing to facilitate public sector transformation and integrated health and social care continues. Numerous regional area multi agency sharing initiatives are seeking guidance and there are significant issues to address.

Outcome:

One area that has continued to be of interest is the use of IT systems that may not be fully DPA compliant. We have met with some of the most problematic IT service providers around issues to do with potential inappropriate sharing of individuals medical records.

Future work:

We will continue to monitor these issues through both complaints raised with us and through working with our stakeholders in this area. Policy

advice is being developed on the status of some of the more problematic IT service provider arrangements in terms of whether they are in fact operating as a data controller or not in terms of the way they handle the data on their system.

We will also engage with NHS England regarding issues in the contracts surrounding the procuring of these IT systems to ensure that future contracts offer more safeguards and guarantees around data protection.

Contact: Andrew Rose

Citizens Jury

We have assisted Manchester University in their sponsored research project to ascertain what the public think about the use of medical records. The vehicle they used was a 'citizen's jury'. We provided evidence to the jury.

Outcome:

The first round of citizens' juries is now completed and they were useful forums for enabling us to get a better understanding of the types of issues that concerned individuals regarding the use of their health data. Furthermore, they allowed us to engage with individuals to better explain to them the realities of what actually happened, particularly in the area of data sharing.

Future work:

Although the first round of citizens juries are finished, we have already been contacted by Manchester University to provide input into two further citizens juries related to Health North. There is also scope for further citizens' juries and we will be looking at the possibility of using them to engage on topics of specific interest to the ICO that need more time consuming and detailed consideration than can be provided by our own citizen reference panel.

Contact: Ian Inman & Rick Syers

6. Business & Industry Sector

Good Practice:

The team conducted a private sector audit at Moonpig.com Limited and sessions were run at the ICO's SME conference, with a focus on records management and the self-assessment toolkit. Work is also well underway on version two of the SME toolkit to deliver greater functionality and additional and updated content.

The Communications audit team continues to conduct audits of CSPs that are subject to data retention notices and is on course to complete audits of all UK based CSPs before the end of the calendar year. During this last quarter the team has been preparing for the ICO's future audit responsibilities under the Investigatory Powers Bill and continues to liaise with the Home Office where appropriate.

Contact: Louise Byers

Cybercrime

Further to the ICO's written submissions, and Christopher Graham's oral evidence, the House of Commons Culture Media and Sport Committee has now published its report *Cyber security: protection of personal data online*.

The report made a number of observations and recommendations for government, industry and the ICO. The Committee's concerns focused on enforcement and sanctions, the information and redress provided to consumers in the event of a cybersecurity breach, the need for developers to ensure systems and applications are secure by design, organisational preparedness, and reporting and transparency as a means to drive up standards.

The Committee raised questions about the ICO's size and ability to handle the volume of concerns received and suggested that Elizabeth Denham should make an assessment of resources and priorities as soon as possible. The Committee responded to ICO evidence by recommending that the ICO should gain additional powers of non-consensual audit and that Sections 77 and 78 of the Criminal Justice and Immigration Act 2008 should be brought into force. The Committee identified there was an urgent need for a mechanism that is easily understood by consumers in order to maintain consumer confidence and inform consumer choices, with particular reference to the ICO's proposed privacy seals scheme.

Outcome:

The Committee has made some positive recommendations addressing ICO concerns raised in evidence. Given conflicting news priorities the report did not receive as much media attention as it might otherwise. Government will need to make a formal response to the consultation. We have already undertaken an analysis of the recommendations and liaised with DCMS officials to ensure they are informed on our position.

Future work:

We will need to formally respond to the Committee. This work is already underway. We should take the report's recommendations into account in our information rights policy work and business planning.

Contact: Garreth Cameron / Abigail Saul

Age verification and children's privacy

The ICO recently responded to a recent DCMS consultation on age verification for accessing online pornographic material.

DCMS's response to the consultation was published in early July 2016, and featured a commitment to bring forward legislation on online age verification; as well as to continue to work with industry players and key stakeholders as part of wider internet safety work. The Digital Economy Bill has now been published, including provisions requiring age verification and creating a regulatory regime for those provisions, including enabling a regulator to tackle third party payment and other service providers where they facilitate a non-compliant website.

Outcome:

There is potential for age verification measures instituted as a result of the Digital Economy Bill to result unintentional privacy implications.

Future work:

We will work with DCMS, Ofcom and other interested parties, as expressed in our consultation response, to ensure that any age verification controls are implemented in compliance with data protection law.

Contact: Garreth Cameron/ Abigail Saul

Fraud registers

NOT FOR PUBLICATION

7. National Regions

7.1 Wales

Welsh Language Standards

Arguably the most significant piece of work undertaken by the Wales office during this quarter was our response to the draft Welsh Language Standards Notice issued by Welsh Language Commissioner in April. The response was submitted at the end of May. The Notice set out around 170 separate standards with which we are likely to have to comply.

While this piece of work was not about information rights per se, a successful outcome – ie the imposition on the ICO of Standards that are reasonable, proportionate and workable – should ensure that our information rights work is not negatively impacted by the additional burden placed on us in order to comply with the Standards.

Future work:

We will receive the final Compliance Notice from the Welsh Language Commissioner at the end of July, at which point an appeals process can commence if necessary. Otherwise the new Standards will apply six months after that date.

Contact: Dave Teague

Voluntary Sector

In April we re-established liaison with the Wales Council for Voluntary Associations ('WCVA') who had recently restructured their IG staff. The meeting was very positive and we agreed to work closely together to improve practices in the voluntary sector in Wales via methods such as workshops, seminars and webinars.

Future work:

Working with the WCVA will give us access to their 4,000 member organisations, as well as to smaller charities that belong to Community Voluntary Councils and Voluntary Centres across Wales. This work will also contribute significantly to the ICO Wales business plan for 2016/17.

Contact: Dave Teague

Health

In 2015 the Wales office and Good Practice team undertook an audit of IG training and awareness in NHS Wales which articulated serious questions about the efficacy of the "Caldicott: Principles into Practice" information governance tool.

Outcomes:

Work is now underway in NHS Wales to develop a more robust approach. We have been involved in discussion of options through the national IGMAG and WIGB committees, and the resulting proposal paper will be going for decision to the WIGB meeting in July. The option preferred by NHS Wales IG Managers is to develop a new on line governance tool that draws on the best elements of the England IG Toolkit but is tailored to Welsh needs and objectives. Welsh IG Managers are also proposing that the tool should require robust evidence that is reviewed annually by each organisation's internal audit and at regular intervals by an appropriate external body.

Contact: Helen Thomas

7.2 Northern Ireland

Championing citizens' rights in partnership with key NI organisations through the ICO NI Citizens Rights Forum

Work includes:

Establishing a 'Citizens Rights Forum' comprised of key stakeholders in the public, private and voluntary sector (including the NI Consumer Council, Trading Standards, the PSNI, the Health and Social Care Board, Citizens Advice and the Older People's Commissioner for NI) with an objective to effectively promote the rights of citizens enshrined within the regulatory remit of the ICO.

Future action:

The Forum is to meet for the first time on 1 July and regularly thereafter. The initial meeting will focus on nuisance calls. Where appropriate, MOU's will be developed with other organisations to ensure effective sharing of information in order for the ICO to take enforcement action or assist with good practice and information campaigns and activities.

Outcomes:

Improved awareness of information rights amongst citizens and a joined up approach amongst stakeholders to help address issues affecting citizens.

Contact: Rachael Gallagher, Shauna Dunlop

Embedding compliance and ensuring privacy by design within the welfare advice sector

Work includes:

Following an initial enquiry from Citizens Advice regarding the transfer of data to partners as part of a government funded project to provide advice to individuals on the impact of Welfare Reform, we advised the partners to conduct a Privacy Impact Assessment to assist data protection compliance.

Future action:

As required. We anticipate that further assistance regarding the PIA's will be sought.

Outcomes:

By adopting a 'privacy by design' approach to the collection and sharing of data, the thousands of individuals across Northern Ireland affected by the overhaul of welfare reform can be assured of the levels of protection given to their information.

Contact: Shauna Dunlop, Rachael Gallagher

Improving information rights compliance across the credit union sector

Work includes:

Working in partnership with the Irish League of Credit Unions, we have agreed to deliver a programme of activities across Northern Ireland to assist credit unions in understanding data protection issues arising from the Credit Unions and Co-operative and Community Benefit Societies Act (Northern Ireland) 2016. We delivered the first workshop on 23 June, which was attended by approx. 70 representatives from credit unions.

Future action:

Further engagement with individual credit unions is planned during the summer, culminating with a sector wide conference in Feb/March 2017.

Outcomes:

Increased understanding of data protection compliance across the credit union sector. Members of credit unions will benefit from improved compliance with information rights law assisted by a privacy by design approach to system development. Successful strategic partnership developed to increase the reach and the impact of the ICO Belfast office.

Contact: Shauna Dunlop

Informing and improving information rights compliance within the community and voluntary sector

Work includes:

Our year long programme in partnership with the NI Council for Voluntary Action continued during this period. We delivered half day sessions on 'Big Data and Open Data' and 'Anonymisation in Practice'. Over 50 organisations attended the workshops and follow up work was completed with individual organisations as required.

Future action:

The programme will continue as planned for the remainder of 2016.

Outcomes:

Improved awareness of information rights compliance across the voluntary and community sector in NI. Improved relationships brokered within the sector. Successful strategic partnership developed to increase the reach and the impact of the ICO Belfast office.

Contact: Rachael Gallagher, Shauna Dunlop

7.3 Scotland

Cross-Sectoral Data Sharing

Delivery of a series of presentations and workshops in conjunction with Policy Hub, throughout Scotland. Multi-sectoral attendees were represented over five sessions in Glasgow, Edinburgh and Aberdeen. We reached some 100 attendees from across all sectors by way of

presentations and a data sharing exercise which received extremely positive feedback.

Future Work:

It is likely we shall work with Policy Hub again on its next seminar series.

Outcomes:

Raised profile of ICO's Scotland Regional Office, as well as being an authoritative source of advice and guidance; continued opportunities for engagement with stakeholders from across all sectors.

Contact: Ken Macdonald/David Freeland/Maureen Falconer

ICO Scotland Annual Conference 2016

This year saw over 100 delegates travel to the Drumossie Hotel, Inverness for the annual conference on the theme of GDPR. Around one-third of attendees were from the private and charity sectors and a greater proportion than normal were from the Highlands and Islands. The speakers were all sourced from within the ICO, principally from Policy Delivery, Strategic Liaison and Enforcement.

Future Work:

Feedback will inform future conferences and other events.

Outcomes:

Raised profile of Scotland Regional Office within "One ICO. Promotion of the ICO as an authoritative source of advice and guidance in the face of change. Continued opportunities for engagement with a wide range of stakeholders.

Contact: Ken Macdonald/David Freeland/Maureen Falconer

Management and Storage of Police Wellbeing Concerns for the Lothians

We were asked to assist NHS Lothian, City of Edinburgh Council and Police Scotland, with the process of forwarding police concern reports once the Children & Young People (Scotland) Act 2014 comes into force on 31 August 2016. We are of the view that the current process is not compliant with the DPA and will be inadequate for the CYPA and the Named Person. We provided advice and guidance on how the concerns identified might be addressed. Police Scotland will take this forward and a

new regime will be devised for procedures before the expected commencement date of 31 August.

Future Work:

Continued advice and guidance to other areas as the new procedures are rolled out.

Outcomes:

Raised profile of ICO as the Regulator of the DPA, as well as being an authoritative source of advice and guidance; opportunities to engage with stakeholders.

Contact: Maureen Falconer

Scottish Parliament New Members Fair

Working with the IG lead at the Scottish Parliament, we spent two days at the Parliament providing DP advice and guidance to the new intake of MSPs as well as registering new and returning MSPs “on site”..

Future Work:

Continue contact with MSPs as and when required.

Outcomes:

Increased opportunity to engage with MSPs and their staff to raise the profile of the ICO.

Contact: David Freeland

8. International

International transfers to the US

Following the publication of the Article 29 Working Party opinion on the draft Privacy Shield Framework in April 2016, which included considerable ICO drafting, legal and analytical input to the conclusions (as well as input to an accompanying analysis of European essential guarantees to assess the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data), the European Commission has resumed negotiations with the United States to try and address the Working Party's concerns.
The revised Privacy Shield is expected to contain at least some of the improvements that the Article 29 Working Party called for however there is no further formal consultative role for the Working Party.

Outcome:

The ICO has continued to provide DCMS with further advice regarding the Article 29 opinion to aid the evaluation.

The revised Shield has been approved by the Article 31 Committee, which is composed of representatives of Member States via their examination procedure.

Next steps:

Adoption of the Privacy Shield is foreseen on 12 July by the European Commission's College of Commissioners.

There is then expected to be a period of implementation before the Shield will enter into force. The ICO will provide further guidance regarding transfers of personal data to the United States once the final details of the Shield are known.

An Article 29 Working Party extraordinary plenary will issue its view on the revised Shield in the summer. While the Working Party's opinion is advisory and not binding, UK data controllers often take such opinions into account in their decision-making. The possibility of a data subject or another entity taking a new case to the CJEU against the Privacy Shield, following the original complaint from Maximilien Schrems that overturned the validity of Safe Harbor, should also be kept in mind.

Contact: Steve Wood/Geraldine Dersley/Naomi Osborne-Wood

European Data Protection Reform

The final texts of the General Data Protection Regulation (GDPR) and the Directive (law enforcement) have been adopted. The GDPR will come into force on 25 May 2018 and the Directive on 6 May 2018.

The ICO has also played a leading role in Article 29 Working Party planning for transition to the European Data Protection Board (EDPB) with its counterparts from other European data protection authorities, notably on the future EDPB engagement with stakeholders, development of policy understanding of Lead DPA, development of processes and templates for cooperation and consistency in chapter 7 and 8 of the GDPR, including a system of mutual assistance between authorities, and work on consistency across the EU in imposition of administrative fines.

Next steps:

The ICO will co-lead workshops with European counterparts to test the concepts introduced in the papers on cooperation and consistency (pending further announcements from government regarding EU referendum follow-up).

Contact: Steve Wood/Iain Bourne/Hannah McCausland

New Europol Regulation

The new Europol Regulation will enter into force on 1 May 2017, increasing the Agency's accountability and strengthening the data protection regime compared with the current EU legal framework in place since 2009 based on an EU Council Decision. A major change will be that supervision of Europol will be carried out by the European Data Protection Supervisor (EDPS) as of 1 May 2017, compared with the current arrangement under the Council of the European Union organising the national governments of the EU.

Outcome:

The ICO was heavily involved in drawing up the terms of reference for the Cooperation Board so that the final terms are acceptable to the ICO.

Next steps:

National data protection authorities, including ICO, will continue to play an important advisory role to the EDPS as part of a Cooperation Board.

Contact: Naomi Osborne-Wood

New Passenger Name Record Directive

A new directive regulating the use of Passenger Name Record (PNR) data in the EU for the prevention, detection, investigation and prosecution of terrorist offences and serious crime was approved in April 2016. It will oblige airlines to transfer passengers' journey-related personal data to national passenger information units for all flights from third countries to the EU and vice versa. Member States also have the option to collect intra-EU flight data from passengers. The UK already operates a long-standing PNR data collection system. This new Directive harmonises the collection of such data across Europe.

The Directive includes data protection safeguards including the mandatory appointment of a data protection officer, greatly reduced retention (6 months) of the full PNR data set and strictly controlled and limited access to that data set after the initial retention period. There is also an explicit prohibition of processing sensitive personal data.

Outcome:

The ICO provided advice to the Home Office at regular intervals during the last months of the negotiations based on the positions that it has heavily influenced over the past few years as a part of the Article 29 Working Party. As a result, the safeguards in the PNR directive have been strengthened to take account of the ICO's/the Article 29 Working Party's views.

Next steps:

The ICO will continue to work with the Home Office and airline carriers on the implementation of the Directive and the associated safeguards including increased notification to data subjects and easier redress mechanisms.

Contact: Naomi Osborne-Wood

GPEN - Global Privacy Enforcement Network

The ICO continues its active participation in the Global Privacy Enforcement Network (GPEN) Executive Committee. GPEN's focus is on upholding individuals' rights more effectively in the global, not just national context by finding ways to improve international (cross-border) enforcement cooperation in practice between GPEN member authorities of which there are now approximately 65.

The emphasis recently has been on improving processes and practices which allow case handling officers at the GPEN member authority

grassroots to quickly and effectively communicate with each other, as well as understand the types of opportunities for synergy that exist with other GPEN members, through training, similar case-handling and enforcement techniques. In May, the European Spring Conference agreed to allow GPEN to organise a session with the 2017 Host of the European Case Handling Workshop to allow European and other GPEN members to analyse cases on a chosen theme to identify best practices.

Contact: Hannah McCausland

Common Thread Network – relations with Commonwealth counterparts

The collection of data protection authorities in Commonwealth countries, known as the Common Thread Network, is continuing to grow and cooperation is continuing to flourish with the aim of fostering sharing of knowledge and good practices and enable capacity building.

Outcome:

The Network has created a dedicated online portal to showcase its activities to any Commonwealth governments and other interested entities from the civil society and the public at large which helps to promote the messages of good data protection practice across the Commonwealth.

Contact: Hannah McCausland/Alain Kapper

International visitors

The ICO received a representative of New Zealand's Office of the Government Chief Privacy Officer from the New Zealand Government's Department for Internal Affairs. Subjects covered were the ICO's policy on overcoming challenges towards information sharing, as well as a showcase of our Good Practice data protection/privacy self-assessment tools for data controllers.

Contact: Alain Kapper

Article 29 Working Party

Significant issues with implications for information rights (where these have not been referred to in other dedicated sections above) include:

- Adoption of an Opinion explaining how to apply the data protection principles to the processing and publication of personal data for transparency purposes in the public sector, in particular when

related to anti-corruption measures and the management and prevention of conflicts of interest. The Opinion addresses issues relating to each of the data protection principles and pays special attention to data subjects' rights and data security. For example, it clarifies when the data subject shall be able to obtain from the certain information from the competent institutions. It should be noted that the Opinion does not cover freedom of information law considerations. The ICO was involved in the work of the sub-group drafting the opinion.

Contact: Hannah McCausland/Jo Pedder

European Spring Conference of Data Protection Authorities

The European Spring Conference of Data Protection Authorities adopted two resolutions at their Conference in May in Budapest.

One resolution addressed trans border flows of personal data, largely related to the EU-US Privacy Shield and data protection authorities' enforcement in relation to the invalidated Safe Harbor.

The other resolution addressed 'new frameworks of cooperation' between data protection authorities across Europe.

Outcome:

At the conference, the ICO was able to share the progress it has made so far on implementing changes for the forthcoming EU data protection reform and recommend common steps that conference members can take together.

Next steps:

The ICO will remain in contact with the DCMS to follow up the resolutions.

Contact: Steve Wood/Hannah McCausland

Schengen SIS II

In April, the SIS II Supervisory Coordination Group (SCG) adopted its programme of work for the period 2016-2018, which recognises the growing need to exchange information in relation to law enforcement and criminal matters. Attention will be paid in that regard to changes in the Schengen border code, Visa code, special rules for alerts on foreign fighters and other sensitive matters. Three further priorities will receive additional attention: a general study on logging in the system, an overview of practices regarding Article 24 alerts (flagging an alert to withdraw its effect in a specific Member State), and a survey of data

retention periods of alerts. A Common Position on the “Deletion of alerts on stolen vehicles” was also adopted by the SCG.

Next steps:

Building on its experience of the recent audit it carried out of the UK SIS coordination unit, Good Practice will participate in the expert on-site visit mission for the evaluation of Malta. The mission is due to take place in September 2016.

The Coordination Group will also continue taking advantage of the recommendations and outcomes adopted from the evaluation of the implementation by Member States of the Schengen Acquis with regards to data protection (known as SchEval).

Contact: Alain Kapper

Customs Joint Supervisory Authority (JSA)

The future of the Customs Information System (CIS) was put into question at the last meeting of the Customs JSA in June 2016 due to the low usage by designated authorities. As regards its immediate future, question was raised on the designation of a new secretariat due to the absence of a new legal basis for the CIS, the reduction in work for the Secretariat and the retirement of the current secretary.

Outcome/Next steps:

The Secretariat of the JSA will draft a letter to send to the three institutions conveying the general message of low usage, and recommending its closure.

Contact: Alain Kapper

Internal Market Information System (IMI)

The IMI Supervision Coordination Group (SCG) comprising all EU data protection authorities met for its second meeting in June 2016, after a two year preparation period at the EDPS and EU Institutions for setting up the new field of work. The Group adopted its rules of procedure and discussed its future programme of work. The number of complaints received by DPAs is relatively low. It was however felt that more information was necessary on the use and performance of the system.

Outcome:

The SCG will work on a questionnaire to be distributed to national IMI coordinators to gain a better understanding of usage within member states and on how the system is monitored by national IMI coordinators.

Contact: Alain Kapper

BIIDPA – British, Islands and Irish Data Protection Authorities

The Data Protection authorities of the British Islands and Ireland (BIIDPA) met in Malta on 21 June. The event was attended by the data protection authorities of Malta, Isle of Man, Gibraltar, the Channel Islands, Ireland and ICO. Coming just one month after the adoption of the EU data protection reform's final legal texts, the focus of the meeting was very much on the application of the new Regulation (GDPR). Members discussed the need, acknowledging the challenging economic climate, to step up contacts to national ministries to secure adequate financial resources to apply the new law, to prepare for and efficiently and effectively fulfil their responsibilities to data subjects set out in the GDPR. Outcome:

BIIDPA will continue to work on ensuring businesses and organisations are able to meet to their obligations under the European data protection framework and to call on relevant governments to make timely decisions to clarify the final shape of the DP framework and the legislative vehicles that will be employed to implement it.

ICO will share any relevant material which BIIDPA partners can use to meet their responsibilities under the new DP framework, including providing advice and raising awareness among businesses and organisations.

Contact: Alain Kapper

9. Enforcement

Direct marketing and nuisance calls

The ICO has continued to prioritise this privacy issue affecting millions of UK citizens. We have stepped up our enforcement action considerably exercising the full range of our enforcement powers and increased our pro-active activities.

Outcome:

We issued five civil monetary penalties totaling £610,000 for contraventions of the Privacy and Electronic Communication Regulations (PECR), by organisations making or sending unsolicited marketing calls and messages.

The largest fine in this quarter was £250,000 against Checkpoint Claims Limited. Other fines included, Nevis Home Improvements for £50,000, Better for the Country/Leave.EU for £50,000, Quigley and Carter Limited for £80,000 and Advanced VOIP Limited for £180,000.

We also served one Enforcement Notice against Central Compensation Office Limited to compel their future compliance with the law. Three Preliminary Enforcement Notices were issued in this period for which we await representations.

We monitored four organisations this quarter which we believe represent risks in relation to adherence to PECR. We held six compliance meetings with organisations in order to tell them to improve their direct marketing practices. Progress will be monitored by the team.

International enforcement engagement and co-operation

The fourth annual GPEN Sweep took place in April and was led by the ICO. Around 30 other Data Protection authorities participated. The topic was the 'Internet of Things' with a focus on accountability. In the UK we considered fitness wearable devices, as well as contacting NHS health trusts to find out more about their usage of connected devices. We also took the topic to the ICO Citizen's Reference Panel to find out more about consumer understanding of the data collected by fitness wearable devices. Global results and follow-up recommendations will be produced during the second quarter.

On 14 June, we announced that we were one of eleven international enforcement authorities which have signed a memorandum of understanding (MoU) committing to share intelligence about unwanted calls and messages. All eleven signatories of the MoU are members of the

London Action Plan group which promotes cross-border intelligence-sharing and cooperation to fight the global problem of spam, scams and unsolicited messaging. The MoU builds on ICO enforcement action to tackle nuisance calls and spam texts.

We have continued to develop new relationships with other relevant regulatory and industry organisations nationally and internationally, including by presenting at the annual International Consumer Protection Enforcement Network (ICPEN) event attended by representatives from 46 jurisdictions.

Data loss incidents

In common with our experiences in 2015/2016, case receipts continue to climb. Over 500 cases were received by the civil team in the first quarter. We forecast that a continuation of intake at this volume will result in receipts of over 2,000 cases by year end, an increase of around 18%. The team continues to ensure that sufficient resources and operating models are in place to respond to this demand.

Outcomes:

Q1 2016/2017 saw the introduction of additional management information categories within the civil team's risk assessment, in relation to cyber-security incidents. This reflects the demand for a more detailed breakdown of incidents and will be used to inform our wider intelligence gathering needs. Over 40 cases from the Q1 intake relate to cyber-incidents, of which cyber security misconfiguration and exfiltration incidents were the most prevalent. The new categories will feature in the Commissioner's Data Security Incident Trends report for Q1, which will be published before the end of July.

In line with previous years' experience and as reflected by the mandatory reporting regime, the Health sector continues to dominate intake. This is followed by the Local Government Sector. The third most prolific sector for intake is General Business; with an increase in receipts reversing the decline in noted in Q4 of 2015/2016.

NOT FOR PUBLICATION

We imposed four Civil Monetary Penalties, totalling £595,000. The penalties were issued to **(1)** Blackpool Teaching Hospitals NHS Foundation Trust following the upload of staff data to a website in error. The data included sensitive personal details such as religious beliefs and sexual orientation (https://ico.org.uk/action-weve-taken/enforcement/blackpool-teaching-hospitals-nhs-foundation-trust/);

(2) The Chief Constable of Kent Police, after sensitive details relating to woman who had accused her partner of domestic abuse were passed to the suspect (https://ico.org.uk/action-weve-taken/enforcement/chief-constable-of-kent-police/); **(3)** Chelsea and Westminster NHS Foundation Trust, following an incident which revealed the email addresses of hundreds of users of an HIV service (https://ico.org.uk/action-weve-taken/enforcement/chelsea-and-westminster-hospital-nhs-foundation-trust/). The notice has since been appealed; **(4)** The Chief Constable of Dyfed Powys Police, after an email disclosure revealed details that could be used to identify registered sex offenders to a member of the public (https://ico.org.uk/action-weve-taken/enforcement/chief-constable-of-dyfed-powys-police/).

NOT FOR PUBLICATION

We issued five fixed penalty notices of £1,000 under the Privacy and Electronic Communication Regulations against communications service providers for failing to report unauthorised disclosures of personal data as a result of security breaches. EE, Alternative Networks Ltd, and Virgin Media all received fixed penalties. The Intelligence Hub produced a new monthly report on these types of breaches which was circulated to ICO policy and operational teams.

Q1 also saw the service of an Enforcement Notice, requiring improvements to staff training and the security of home working measures, to West Dunbartonshire Council. The Notice is currently subject to appeal.

Two undertakings, requiring improvements in the data compliance practices of Wolverhampton City Council and the Health and Social Care Information Centre (HSCIC) were signed in Q1.

The HSCIC undertaking, which followed an investigation into the application of opt-outs offered to patients ahead of data being shared with other organisations, secured improvements in a key and emerging information rights area. The undertaking can be accessed at:

https://ico.org.uk/action-weve-taken/enforcement/health-and-social-care-information-centre-hscic/

NOT FOR PUBLICATION

Finally, Q1 saw the publication of the Department of Culture, Media and Sport Select Committee's report into cyber security – available at:

http://www.publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/14802.htm.

Criminal investigations and prosecutions

The number of prosecutions for a range of criminal offences continues to rise. This reflects the increased resources introduced last year and the sharper focus that we are able to apply to privacy issues and concerns reported to us or identified by us.

In Quarter 1 we expanded capability and capacity in respect of RIPA telecoms applications, by developing a further team member as a trained Telecoms SPoC. The delivery of the Advanced Certificate in Investigatory Practice began in Quarter 1 with a number of staff studying for the qualification.

During this period there were nine telecom applications submitted, eight were granted and one was refused by the Senior Responsible Officer (SRO). The Telecom SPoC has assisted the SRO with preparing a case to support the retention by the ICO, of powers for the minor users of communications data.

We were asked to provide advice on 103 cases with a potential criminal breach during Quarter 1. Of these, 52 cases were allocated for further investigation. Progress continues to be made against all legacy cases following the impact of Op Spruce.

We executed one search warrant during this period in relation to an ongoing case involving Lex Autolease. A Number of items were seized that are currently being examined by our forensic service provider.

NOT FOR PUBLICATION

A case contrary to s56 DPA against Minera Tyres is proceeding to prosecution, the defendant in that case elected for trial at Crown Court. A prosecution under s55 DPA against David Lewis on the 7th April resulted in a £300 fine, with costs of £614.14 and a £30 victim surcharge. On the 26th May Mark Lloyd was prosecuted under s55 DPA receiving a £300 fine with £405.98 costs and a £30 victim surcharge. Although the team were able to progress a s77 FOIA allegation within the statutory time limit, The Legal Team determined that it was not in the public interest to prosecute.

During this quarter there were a further 34 Non-Notification cases referred by the Customer Contact Registrations Team. Of the ongoing cases 30 were closed ‘No Further Action’, 29 subsequently notified and 7 cases were referred to Legal.

Keurboom Communications Limited and its Director, Mr Gregory Rudd, were prosecuted for failing to respond to a Third Party Information Notice. Both pleaded guilty. The company was fined £1,500 with costs of £493.95 and a victim surcharge of £120. Rudd was fined £1,000 and also ordered to pay costs of £493.95 with a victim surcharge of £100.

We prosecuted Getwork2day Limited and Money Saving Champions Limited for non-notification offences. Getwork2day Limited did not attend Court and were fined £500 in their absence, with £951.79 in costs with a £50 victim surcharge. Money Saving Champions pleaded guilty and were fined £350, with £493.75 in costs and a victim surcharge of £35.

At the present time, two further prosecutions for non-notification or related DPA offences are scheduled to take place in the next quarter.

Next quarter we will continue to work with partner agencies. Operation Brenta was commenced following a referral by the Insurance Fraud Bureau. This investigation focusses on potential offences under S55 DPA involving fraudulent mandates from a claims management company to obtain data of persons involved in road traffic collisions. It is anticipated that a file will be submitted to Legal during Quarter 2. We are currently liaising with the Retail Motor Industry Federation regarding data leaks from garage repair businesses; this has attracted media attention at a National level.

As part of the ICO 'looking for trouble strategy' the CrIT conducted a proactive operation in Quarter 1 (Bernia).

NOT FOR PUBLICATION

During w/com 16th April officers from the CrIT visited 16 premises with outcomes of 5 'No Further Action', 9 being monitored for Principle 1 issues, and 2 referrals for Non-Notification.

Operation Urner was launched following a referral from ACRO of 2500 potential enforced Subject Access Requests. Contact was made with a number of organisations to assess compliance with the DPA, and where appropriate a change in practice and policy was advised. This approach was deemed appropriate and proportionate given the volume, and as there was no identified detriment to individual data subjects. Whilst the Operation is currently being finalised a number of organisations have changed their practices and ACRO have refined their processes to better identify offences.

Operation Spruce

The investigative priority remains to be Operation Spruce. Progress continues to be made following the submission of the first file to the ICO Legal team during Quarter 3 2015/16. A prosecuting decision is imminent following some additional work on the case during Quarter 1. Investigations into nine other clients continue with further files to be submitted over the course of 2016.

NOT FOR PUBLICATION

A disclosure officer has been recruited on a fixed term contract to assist with case preparation.

Engagement activities and service improvements

Improvements to the online reporting tool now allow people to report multiple unsolicited marketing calls or messages.

We have now integrated specialist software to improve our analytical abilities, as well as improving the existing nuisance calls/texts reporting tool during this quarter. We have also introduced new procedures for open source research to enable improved intelligence gathering, whilst ensuring compliance with relevant legislation.

We continue to publish the quarterly data security incident trends report as well as the monthly nuisance calls and messages threat assessments on our website. We updated our activity report in relation to cookies. We shared intelligence with other regulatory and law enforcement organisations to support our enforcement activity and their priorities.

Outcomes:

We attended a ‘nuisance calls summit’ on 29 June arranged by the Scotland Government, and set out a number of actions that could be taken to improve reporting of concerns, and co-ordination of enforcement action. The Minister leading the summit agreed to support the actions.

In early June, the ICO supported Trading Standards Scotland in a ‘week of action’ in order to co-ordinate messaging around planned enforcement action and take-up of the Telephone Preference Service. The ICO publicised enforcement action during the week in respect of two related monetary penalties and an enforcement notice.

Under the Victims Code complainants have a right to request a review of a decision not to prosecute. This right was exercised on four occasions; in

each case the original decision was upheld with one of the cases considered by Counsel at the request of Legal.

In April, the Civil Team delivered a series of compliance workshops to small and medium enterprises as part of the SME Conference held in Birmingham. The workshop, which comprised of an interactive desk-top session designed to mimic the aftermath of a data breach, gave delegates an opportunity to discuss their experiences and to share best practice.

In June, the Civil Team delivered a webinar – designed to raise awareness of the risks of failing to ensure that adequate security measures are undertaken when processing personal data in the legal sector was delivered during the Bournemouth Law Society Conference. The webinar is due to be repeated in July to a wider sector audience.
Next Quarter:

- We will progress Operation Spruce by driving performance through the completion of actions and aim to submit prosecution advice files to the Legal team.
- We will continue to progress the legacy cases to completion and seek to increase the volume of prosecutions and cautions.
- We will continue to prioritise our investigations and activities to maintain focus on effective enforcement of the PECR.
- We will improve our understanding of the 'Data Cycle' operating in the direct marketing sector through focused analysis of information obtained during Op HIDA.
- Recruitment of additional Analysts in the Intelligence Hub and new Technical Investigators in the Civil Investigations Team will be completed. The investigators will form a new team with specific responsibility for the investigation of cyber-security incidents and other complex technological cases.
- We will conduct a review of the digitisation scheme used at Liverpool Crown Court with Strategic Liaison to better understand the technical advances made in the police and criminal justice sector. This is an area which we continue to see a high number of disclosure in error cases.
- We will progress our cases into the marketing activities of charities we believe have contravened the Data Protection Act and PECR.
- We will review our current enforcement approach in relation to breaches of the PECR and use of Cookies to ensure that we are targeting non-compliant organisations causing the most serious detriment to consumers.
- We will continue to develop the ICO's Horizon Scanning and 'Looking for Trouble' strategies by actively seeking new sources of intelligence and strengthening or intelligence sharing arrangements with other regulatory and law enforcement organisations to support our enforcement activity.

- Global findings from the 2016 GPEN Sweep will be collated and announced during quarter two. We will also produce an internal report into the findings to decide on the next steps to be taken.
- We will continue to pursue a number of new initiatives and projects in coordination with members of the London Action Plan (LAP) ahead of the next meeting in October. Ongoing projects include identifying intelligence contacts, combining expertise and training materials and continuing to develop the first LAP Sweep, where members will cooperate on the theme of affiliate marketing to develop a global understanding of the practice and identify opportunities to coordinate activity.
- We will follow up on agreed actions from the International Enforcement Cooperation Event held in March, including working with the Canadian Office of the Privacy Commissioner to revise the International Enforcement Cooperation Handbook ahead of the next International Conference in October, and further develop opportunities for international enforcement cooperation.
- We will develop the teams through the delivery of the Advanced Certificate in Investigatory Practice, and BCS Data Protection course.
- Finally, the team will continue to make preparations to welcome the new Commissioner, Elizabeth Denham.

Contact: Steve Eckersley

10. Performance Improvement

The first quarter of 2016/17 has been challenging for the department because of significant increases in intake. DP complaints/concerns cases are up just under 25% when compared to the same quarter last year and FOI cases are also up nearly 20% on those received last year. It has been the highest intake this quarter since 2009. As a result the department has not been able to exceed intake with closures. This is despite some good overall productivity returns. Inevitably overall caseloads have increased. This has not directly impacted on the service that we have been able to provide at the moment, with over 70% of cases coming to us being concluded within 3 months of receipt, but there is a risk that it will do so as the age of cases unresolved increases.

In an attempt to increase capacity we intend to introduce a seventh Improving Practice Group that will have responsibility for a significant number of data controllers and predominantly across those in the private sector. Although case increases are seen across the board, the general business sector is the one that requires most assistance. We have not as yet identified a significant individual cause of the increase in complaints casework although we have some anecdotal evidence of more claims management companies utilising subject access as a way to further their business. We have been successful in recruiting a new Group Manager for the department and been able to promote from within to cover other impending management departures. We are also actively underway with recruitment for team manager and case officers to ensure that the new department structure can operate as envisaged. We are also offering overtime at weekends, both in the office and for those available to homework, in an attempt to mitigate the impact for those that require our help.

As well as our routine data protection and freedom of information casework we have continued to assess search engine cases for those that want the results to be removed. There were 91 new cases this quarter and we were able to conclude 90. Lower level self-reported incidents are also being handled with in the department and we have dealt with an additional 160 cases at the time of writing.

Formal freedom of information monitoring activity continues. Trafford Council was advised it is to be subject to formal monitoring for the period 1 May to 31 July 2016 because of its failure to provide sufficient responses within statutory timelines. However it is good to note that following an extended period of monitoring and sustained improvement the Ministry of Justice is no longer required to submit monitoring returns. We have continued to work closely with the Metropolitan Police Service about service levels. They have committed additional staff to help

improve turnaround times, however, they also highlighted that they have been experiencing a significant increase in volumes of requests.

Following work with the NI Departments, and their restructure, we had follow up meetings with the Executive Office (formerly OFMDFM), the Department of Finance (formerly the DFPNI) and the Department of Health. These meetings and additional correspondence resulted in a number of significantly overdue requests (potential enforcement notice cases) being cleared. In addition the Department of Finance maintained sufficient improvement to enable its formal monitoring to be concluded. As follow up to previous monitoring activity, the Commissioner visited Stormont and addressed the Permanent Secretaries Group, on 17 June 2016, commenting positively on their Departmental and staff performance and their co-operation with the ICO.

There have been over 5,500 individual cases concluded this quarter. The following are examples of cases or actions that have directly resulted in improvement of information rights practices, following from concerns raised by the citizens.

Fifteen specific actions have been agreed with local councils across the country. Highlights include an action plan produced for Cheshire East, after issues had been identified in a number of cases where inaccurate data had been found to be the root cause of a number of complaints. Meetings have been held in Wilmslow with Liverpool City Council to draw attention to a trend that had been seen in the way in which delays in their responses to both the ICO and the requestors' original requests. The follow up meeting allowed Liverpool to demonstrate the changes in the training they had implemented and a commitment to improve, which has been reflected in subsequent correspondence.

Advice has also been provided to Essex, Derby and Cumbria as a result of issues we were able to reflect improvement possibilities and a range of training and resources has been applied in all three to mitigate future occurrences.

We have continued to work in providing advice to councils looking to implement CCTV in taxi cabs. In what is a grey area of the legislation, we have also had meetings with the Surveillance Camera Commissioner who have in turn clarified their role in this regard. They have also taken on board the need to refer related concerns to the ICO where they feel that their own responsibilities have come to an end and only DP issues remain.

This quarter we have had cause to liaise directly with Royal Band of Scotland regarding multiple concerns raised by a Claims Management Company alleging failure to respond to subject access requests. We have

also liaised with the CMC regulator on this specific issue and the CMC in question will be audited over the next few weeks.
A concern was raised about Scottish Power (SP) processing inaccurate information. SP initially confirmed that they retained personal data indefinitely following account closure. Further investigation delivered contradictory messages about retention periods. Once the matter was escalated it was confirmed that changes will now be applied to ensure that following account closure no unnecessary personal data will be retained.

JD Sports failed to cease marketing after receiving a section 11 request. We engaged with them to give advice and guidance, following our intervention they have changed their marketing practices and provided a 'preference centre' where customers can change their marketing preferences and unsubscribe at any time.

Nationwide used their Annual General Meeting literature to include marketing materials to customers. We asked them to cease this practice however they maintained that their literature wasn't marketing material. The case was referred to Enforcement and following this the literature was amended to remove the marketing.

We met with NXET trains to advise on the implications of the potential use of body worn cameras for their staff.

Two staff attended the Property Management Unwrapped Conference at Royal Holloway where a session was delivered on the requirements of the DPA and compliance with SARs. A trade stand was used to deliver further messages at breaks and lunch times.

We met with Lloyds Banking Group for a quarterly meeting to levels of compliance and other general DPA issues.

We attended the Scottish Financial Services Forum and delivered a Subject Access Request session at the SME Conference in Birmingham, delivering advice to 200+ delegates. We then delivered a webinar version of this a week later to 1000 online delegates.

Case officer from Performance Improvement met with representatives of the Foreign and Commonwealths FOI Team and discussed a range of issues relating to how we investigate FOI cases. The FCO were advised about a number of ways in which they could provide better submissions to us in respect of complaints we have received about them along with general guidance about handling requests.

The department also met with senior FOI request handlers from the Cabinet Office. We covered particular problems related to cases which cover FOI sections 23 and 24 (security bodies/national security) – ICO access to the information; letters of assurance; paucity of arguments; delayed responses to ICO. Solutions were suggested which require further consideration by Cabinet Office.

The above examples are not exhaustive and simply provide a sample snapshot of the improving practice activity undertaken in the quarter.